International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 11
July2016

Delegating Public Auditing and Invigorate Data Storage in Public Cloud

[1]A.SWAPNA JAYANTHI, [2] Mrs.N.SUJATHA

[1] M.Tech(CSE) from JAGRUTI INSTITUTE OF ENGINEERING AND TECHNOLOGY

[2] Associate Professor, Department of Computer Science and Engineering, JAGRUTI INSTITUTE OF ENGINEERING AND TECHNOLOGY, Telangana State, India.

ABSTRACT:

In cloud computing the data owners will use storage service to outsource their sensitive data and whenever they need they can download from the cloud but due to the privacy challenges protecting data from outside or inside attacks will leads to problem to the data owner. In order to check remote data the data owner need to verify the data periodically and if any failures or modifications identified, then he has to remove old data and he has to upload new data to the cloud this will leads to the burden on the data owner and if data owner use PDP (Provable Data Possession) model it will audit in single server. To overcome the problems and to remove burden on the data owner, in this paper we are proposing MBR (Minimum Bandwidth re-generating codes) and MSR (Minimum storage regenerating code) to securely repairing the block in cloud.

Keywords: Public Auditing , Proxy ,Block regenerator , privacy preserving.

INTRODUCTION:

Cloud computing providing the resource pay-as-you goes whenever any organization need any resource without purchasing the required resource, the organization can access remotely as rental basis, and cloud providing so many services like Software as a service, Platform as a service and Infrastructure as a service. Among these three services Iaas is top on cloud. And cloud providing many features to the users among some features is like Scalability, availability, Maintenance, Data integrity etc. using cloud the user can store or upload data to the cloud and when ever required he can download. Providing security to the data is critical important issue in cloud.

BACKGROUND WORK:

In cloud computing generally data owner can store his data to the cloud and when ever required he can download from cloud ,but lot of data owners assuming there data is not secure so in order to provide security to the data the cloud must auditing to the user .when ever user assume data is modified then he can check the integrity of his data , for this cloud providing TPA(Trusted party

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 11
July2016

Auditor) here the TPA will check the data integrity in cloud. But if any data changes in the cloud

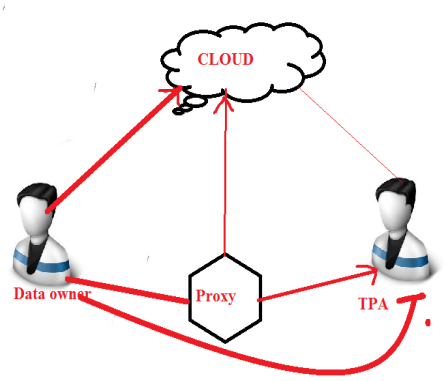
The data owner has to remove his old data in cloud and he has to upload new data to the cloud again so this process will repeat when ever data changes in the cloud it will leads to the burden to the data owner and communication problem . so in order to resolve above issue we are introducing proxy. In this scenario the data owner will upload the file to the cloud and before uploading to the cloud he has to encrypt the file and the meta information he will send to the cloud and same way he will store keys and data into proxy ,if any data modification occurs proxy will replace the data into the cloud.

POR(Proof of Retrievability Model):

This model will provide proof to the data , the TPA will implement this model and the auditing result he will send to the data owner.

PROPOSED WORK:

To overcome existing problems in this paper we are proposing public auditing protocol , the system model implemented based on Data ower , Data User , Cloud ,TPA and Proxy.



Public Auditing Model:

Setup: data owner will generate Key pair , one is Msk and PK.

Encryption: this step run by data owner to encrypt the file using public key , in this step in put is plain text and output is cipher text.

Delegation: this step run data owner in order to share keys to proxy and TPA.

Auditing: this step run by TPA in order to check the integrity in cloud , Input is Challenge to the cloud and output is the cloud will return auditing result.

Regenerate code: this step run by Proxy when ever modifications occurs in cloud it will replace the block in cloud.

CONCLUSION:

In this paper we implemented Regenerating code with public auditing. And the data owner can delegate his privileges to Proxy , now whenever any modification notified by TPA the proxy will replace in cloud. And to provide data integrity we are using

encryption process and Auditing will delegate to the TPA. The authenticator can competently assign to the proxy. Whenever data is modified

REFERENCES:

[1] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil

pairing," Journal of Cryptology, vol. 17, no. 4, pp. 297–319, 2004.

[2] A. G. Dimakis, P. B. Godfrey, Y. Wu, M. J. Wainwright, and K. Ramchandran,

"Network coding for distributed storage systems," Information

Theory, IEEE Transactions on, vol. 56, no. 9, pp. 4539–4551, 2010.

[3] T. Ho, M. M´edard, R. Koetter, D. R. Karger, M. Effros, J. Shi, and

B. Leong, "A random linear network coding approach to multicast,"

Information Theory, IEEE Transactions on, vol. 52, no. 10, pp. 4413–

4430, 2006.

[4] D. Boneh, D. Freeman, J. Katz, and B. Waters, "Signing a linear

subspace: Signature schemes for network coding," in Public Key

Cryptography–PKC 2009. Springer, 2009, pp. 68–87.

[5] D. Boneh and M. Franklin, "Identity-based encryption from the weil

pairing," in Advances in CryptologyłCRYPTO 2001. Springer, 2001,

pp. 213–229.

[6] A. Miyaji, M. Nakabayashi, and S. Takano, "New explicit conditions

of elliptic curve traces for fr-reduction," IEICE transactions on fundamentals

of electronics, communications and computer sciences, vol. 84,

no. 5, pp. 1234–1243, 2001.

[7] R. Gennaro, J. Katz, H. Krawczyk, and T. Rabin, "Secure network

coding over the integers," in Public Key Cryptography–PKC 2010.

Springer, 2010, pp. 142–160.

[8] S. Goldwasser, S. Micali, and R. Rivest, "A digital signature scheme

secure against adaptive chosen message attacks," SIAM Journal of

Computing, vol. 17, no. 2, pp. 281–308, 1988.

[9] P. S. Barreto and M. Naehrig, "Pairing-friendly elliptic curves of prime

order," in Selected areas in cryptography. Springer, 2006, pp. 319–331.

[10] Y. Deswarte, J.-J. Quisquater, and A. Sa¨ıdane, "Remote integrity checking,"

in Integrity and Internal Control in Information Systems VI.

Springer, 2004, pp. 1–11.

A.SWAPNA JAYANTHI is pursuing M.Tech degree in, Computer Science and Engineering from Jagruti Institute of Engineering and Technology, Telangana State, India.

Mrs.N.SUJATHA is presently working as Associate Professor in, Department of computer science and engineering, Telangana State,India.She has published several research papers in both International and National conferences and Journals.